UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CRIMINAL ACTION NO. 11-10294-GAO

UNITED STATES OF AMERICA

v.

DAVID KEITH,
Defendant.

OPINION AND ORDER
November 5, 2013

O'TOOLE, D.J.

The defendant, David Keith, is charged with distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and possessing and accessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). He has moved to suppress physical evidence and statements obtained as the result of a search of his residence by the Massachusetts State Police pursuant to a warrant.

The application for the warrant relied on two distinct sources of information for a showing of probable cause. First, in December 2009, the National Center for Missing and Exploited Children ("NCMEC") made available to the Massachusetts State Police a "CyberTipline" report indicating that a computer that eventually was linked to the defendant's residence was likely the source of an emailed file that contained what appeared to be child pornography meeting the federal criminal definition.[1] Second, on July 29, 2010, employees of a Staples store in New Hampshire notified local police that a laptop computer left for repair contained files with filenames apparently describing child pornography. The work order for the Staples laptop listed the defendant's name and his residential address in Haverhill, Massachusetts. When later questioned by the police in New Hampshire, the defendant admitted both that the Staples laptop was his and that he had seen and downloaded

[1] It appears that other similar reports were subsequently made available to the State Police. The parties have focused only on the December 2009 report, identified by the number 759801, and so I do likewise.

files depicting images of children as young as eight years old engaging in sexual activity. The New Hampshire police ultimately shared with the Massachusetts State Police information they had gathered in their investigation, including some evidence from a warranted search of the laptop. Relying on both the NCMEC CyberTipline report and the information from the New Hampshire police, the Massachusetts State Police applied for and obtained a search warrant for the defendant's residence, which was executed on September 17, 2010. The search yielded incriminating information, and the defendant also made incriminating admissions after having been advised of his Miranda rights.

## I. The CyberTipline Report

The following factual findings are based on the parties' written submissions and testimony given at an evidentiary hearing.

America Online ("AOL"), which may be described variously as an electronic service provider ("ESP") and an internet service provider ("ISP"), provides an email service for subscribers. To prevent its communications network from serving as a conduit for illicit activity, AOL systematically attempts to identify suspected child pornography that may be sent through its facilities. It uses an Image Detection and Filtering Process ("IDFP") of its own devise which compares files embedded in or attached to transmitted emails against a database containing what is essentially a catalog of files that have previously been identified as containing child pornography.

Commonly, AOL may be alerted that an image or video file being transmitted through its facilities likely contains child pornography by a complaint from a customer. When AOL receives such a complaint, an employee called a "graphic review analyst" opens and looks at the image or video file and forms an opinion whether what is depicted likely meets the federal criminal definition of child pornography. If the employee concludes that the file contains child pornography, a hash value of the file is generated automatically by operation of an algorithm designed for that purpose. A hash value is an alphanumeric sequence that is unique to

a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Consequently, once a file has been "hashed," a suspected copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value.

AOL maintains a "flat file" database of hash values of files that AOL has at some time concluded contain child pornography. It does not maintain the actual files themselves; once a file is determined to contain child pornography, it is deleted from AOL's system. When AOL detects a file passing through its network that has the same hash value as one in the flat file database, AOL reports that fact to NCMEC via the latter's CyberTipline. By statute, an ESP or ISP such as AOL has a duty to report to NCMEC any apparent child pornography it discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyperTipline report transmits the intercepted file to NCMEC, but no AOL employee opens or views the file. AOL's decision to report a file to NCMEC is made solely on the basis of the match of the hash value of the file to a stored hash value.

A CyberTipline report is typically created by direct upload to NCMEC's server through a facility made available by NCMEC to an ESP such as AOL specifically for that purpose. After a report is received, a NCMEC analyst opens and views the file to determine whether its content meets the federal criminal definition of child pornography. If it is determined that the file contains child pornography, the NCMEC analyst queries the email sender's internet protocol ("IP") address using conventional "open source" search engines to try to identify the sender's geographic location, as well as the ISP through which the sender accesses the internet. When the general geographic location and the relevant ISP for the computer of interest have been determined, the NCMEC analyst adds the report containing the file to a database that is accessible only to law enforcement agencies in the identified geographic location via a virtual private network ("VPN") that is dedicated to that use.

In this case, AOL identified a suspect file in an email sent on November 26, 2009. The following day, AOL uploaded a CyberTipline report that contained the file to NCMEC's server. In accordance with its practice, no AOL employee opened or viewed the file before it was forwarded to NCMEC. Rather, it was forwarded solely because its hash value matched a hash value in AOL's flat file database. Nothing is known about how the file came to be originally hashed and added to the flat file database, except that it was AOL's practice to hash and add to the database either the hash value of any file that was identified by one of its graphic file analysts as containing child pornography or a hash value similarly generated by a different ESP or ISP and shared with AOL.[2]

After the file was received at NCMEC, an analyst opened and examined the image file, determined that it met the criteria for classification as child pornography, investigated the IP address from which the offending email originated, and determined that the IP address was located within Massachusetts. NCMEC then created the CyberTipline report and made it accessible to law enforcement personnel in Massachusetts through the dedicated VPN, along with information about the email sender's IP address and ISP. Subsequently subpoenaed records from the ISP associated the IP address with a computer at the defendant's residential address in Haverhill, Massachusetts. The Massachusetts State Police also independently matched the IP address to the defendant's address.

## II. NCMEC and Its CyberTipline

According to a statement on its website, NCMEC

> was established in 1984 as a private, nonprofit 501(c)(3) organization. NCMEC works in partnership with the U.S. Department of Justice to help law enforcement find missing children, eliminate child sexual exploitation and prevent child victimization.

[2] AOL and other similar electronic service providers share with each other the hash values of suspected or identified child pornography. It is possible that the hash value of a suspect file was initially generated by another provider and then shared with AOL.

About Us – Congressional Authorization, NCMEC, http://www.missingkids.com/Authorization (last visited Nov. 4, 2013). The "partnership" is reflected in an explicit statutory finding by the United States Congress:

> The Congress finds that–
>
> * * *
>
> (8) the Office of Juvenile Justice and Delinquency Prevention administers programs under this chapter through the Child Protection Division, including programs which prevent or address offenses committed against vulnerable children and which support missing children's organizations; and
>
> (9) a key component of such programs is the National Center for Missing and Exploited Children, which–
>
> (A) serves as a national resource center and clearinghouse;
>
> (B) works in partnership with the Department of Justice, the Federal Bureau of Investigation, the United States Marshals Service, the Department of the Treasury, the Department of State, the Bureau of Immigration and Customs Enforcement, the United States Secret Service, the United States Postal Inspection Service, and many other agencies in the effort to find missing children and prevent child victimization; and
>
> (C) operates a national network, linking the Center online with each of the missing children clearinghouses operated by the 50 States, the District of Columbia, and Puerto Rico, as well as with international organizations, including Scotland Yard in the United Kingdom, the Royal Canadian Mounted Police, INTERPOL headquarters in Lyon, France, and others, which enable the Center to transmit images and information regarding missing and exploited children to law enforcement across the United States and around the world instantly.

42 U.S.C. § 5771. To support this work of the Center, Congress has mandated funding for the Center by means of annual grants administered through the Office of Juvenile Justice and Delinquency Prevention of the Department of Justice. See id. § 5773(b). One of the purposes of the annual grant is specifically to support NCMEC's CyberTipline:

> The Administrator shall annually make a grant to the Center, which shall be used to–
>
> * * *
>
> (P) operate a cyber tipline to provide online users and electronic service providers an effective means of reporting Internet-related child sexual exploitation in the areas of–

> (i) possession, manufacture, and distribution of child pornography;
>
> * * *
>
> and subsequently to transmit such reports, including relevant images and information, to the appropriate international, Federal, State or local law enforcement agency for investigation;
>
> * * *

Id. § 5773(b)(1). As noted above, the CyberTipline is supported by the statutory mandate that any ESP that discovers what appears to be child pornography must report that fact and its surrounding circumstances to the CyberTipline. 18 U.S.C. § 2258A(a). A knowing failure by an ESP to make such a report is punishable by a fine. Id. § 2258A(e). When it receives such a report via the CyberTipline, NCMEC must forward it to an appropriate federal law enforcement agency, and is authorized to do likewise with respect to state law enforcement agencies. Id. § 2258A(c).

According to NCMEC's annual report, for the year ending December 31, 2012, NCMEC received government contracts and grants slightly in excess of $36 million, approximately 70% of its total revenue for the year from all sources. 2012 Annual Report, NCMEC, www.missingkids.com/en_US/publications/NC171.pdf (last visited Nov. 4, 2013). It also receives annual donations from private citizens. For 2012, private contributions were approximately $7.7 million, a little over 15% of total revenue from all sources. Id.

In addition to the CyberTipline, NCMEC also administers a number of other programs relating to missing and exploited children which are not directly relevant to the issues presented in this case.

## III. Expectation of Privacy in the Contents of Emails

The defendant attacks the inspections of his intercepted email by both AOL and NCMEC respectively as violations of his right "to be secure in [his] . . . papers[] and effects, against unreasonable searches and seizures" guaranteed by the Fourth Amendment. A "search" for purposes of the Fourth Amendment occurs when there has been a governmental intrusion into a place or thing as to which a person has a reasonable expectation of

privacy. Put another way, the inquiry is whether the defendant had a subjective expectation of privacy in the place or thing that society recognizes as reasonable. Kyllo v. United States, 533 U.S. 27, 33 (2001).

Email has become one of the most common forms of communication, but courts have yet to come to a consensus regarding whether and to what extent a sender has, for Fourth Amendment purposes, a reasonable expectation of privacy in email committed to the custody of an ISP. See, e.g., Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010), aff'd, 132 S. Ct. 1497 (2012) ("[W]hether [the defendant] had a reasonable privacy expectation in the contents of his personal emails sent voluntarily through that third-party ISP, are complex, difficult, and 'far-reaching' legal issues") (collecting cases). There are some perhaps useful analogs from other methods of transmitting communications. So, for example, while there is not a reasonable expectation of privacy in the matter on the outside of a mailed envelope, there is as to the letter sealed inside, see Ex Parte Jackson, 96 U.S. 727, 733 (1877), and while there is not a reasonable expectation of privacy in the numbers dialed from a telephone, see Smith v. Maryland, 442 U.S. 735, 745 (1979), there is as to the conversation itself, see Katz v. United States, 389 U.S. 347, 352 (1967). Following the principles at work in these and similar cases, one might conclude that a sender of emails has a reasonable expectation of privacy in some aspects of the email, such as the contents of the message including embedded or attached files, but not in other aspects, such as the address header and various metadata.

In any event, the government has not taken the position that the defendant lacked a legitimate privacy interest in the contents of the emailed file, and so it is assumed for present purposes that he had such an interest. That being so, any governmental invasion of that privacy interest would be a "search" for Fourth Amendment purposes.

## IV. Private or Governmental Search?

"The Fourth Amendment's protection against unreasonable searches and seizures applies only to government action and not to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the government." United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009) (citations and internal quotation marks omitted). The defendant argues that neither AOL nor NCMEC was acting as a private party in screening and examining the email file because each was acting under a statutory duty or compulsion and thus must be considered to have been effectively a government agent. Therefore, he contends, their searches are to be regarded as having been conducted by the government for purposes of enforcing the criminal law and thus were subject to the requirements of the Fourth Amendment.

Under First Circuit precedent, whether a private party is acting effectively as an agent of the government in conducting a search is evaluated against three principal factors: (1) "the extent of the government's role in instigating or participating in the search"; (2) "[the government's] intent and the degree of control it exercises over the search and the private party"; and (3) "the extent to which the private party aims primarily to help the government or to serve its own interests." Silva, 554 F.3d at 18.

AOL's comparison of the hash value of the file transmitted from the defendant's computer with its database of stored hash values of files thought to contain child pornography was not a search conducted by or on behalf of the government. None of the so-called "Silva factors" are present. Contrary to the defendant's suggestion, AOL is not required by law to monitor email traffic for possible child pornography, 18 U.S.C. §2258A(f), but only to report it when it is found, id. § 2258A(a). The government exercises no control over AOL's monitoring of its network. Most importantly, the evidence considered on the present motion established, and I find, that AOL is motivated by its own wholly private interests in seeking to detect and deter the transmission of child pornography through its network facilities. An AOL representative testified at the evidentiary hearing held on the present motion that AOL had an important business reason for its IDFP filtering process:

> We found that, again, providing a safer, more family-friendly environment for our users sustains our ability to keep our members. We've noticed when members call and say, "I want to discontinue my AOL service," we usually ask them why. And there are many reasons why somebody may want to leave, but one of these that we're routinely concerned about is objectionable content sent to them through our servers by other members or other Internet users. So they end up leaving AOL because of this bad content. So as a business, we would like to actually keep the members who complain about it and have a countermeasure against those who do it.

(Tr. of Evidentiary Hr'g at 67-68 (dkt. no. 53).) This legitimate business interest is distinct from the government's interest in prosecuting crime, and the Silva factors are not met.[3] Cf. United States v. Cameron, 699 F.3d 621, 637-38 (1st Cir. 2012) (holding that Yahoo!, Inc. did not act as a government agent in searching the defendant's email and sending reports to NCMEC).

On the other hand, NCMEC's examination of the file uploaded by AOL to the NCMEC CyberTipline was a search conducted for the sole purpose of assisting the prosecution of child pornography crimes. NCMEC's goal in operating the CyberTipline is a worthy and laudable one, but it is one that it pursues in "partnership," 42 U.S.C. § 5771(9)(B), with the government. Unlike AOL, which monitors its email traffic to serve its own business interest, NCMEC's operation of the CyberTipline is intended to, and does, serve the public interest in crime prevention and prosecution, rather than a private interest.

The Silva factors are satisfied. Through congressional authorization and funding of the CyberTipline, the government "instigat[es]" such searches. Silva, 544 F.3d at 18. A statutory provision requires NCMEC to report discovered child pornography to federal law enforcement, and another encourages similar reporting to state and foreign law enforcement agencies. 18 U.S.C. § 2258A(c)(1)-(2). This requirement addresses the "control" factor identified by the First Circuit. Silva, 554 F.3d at 18. Finally, the CyberTipline serves no private purpose for NCMEC separate from assisting law enforcement, the third Silva factor. Id.

[3] The "search" of the defendant's laptop computer by Staples employees in July 2010 was also clearly a private search, one in fact invited by the defendant's delivery of the machine to them for their examination. The defendant does not contend otherwise.

While not directly addressing the question presented here, the First Circuit has noted that NCMEC reviews suspected files and "conducts an online search regarding the provided suspect information . . . aimed at identifying the appropriate law enforcement agency with jurisdiction to investigate the suspected child pornography activity." Cameron, 699 F.3d at 633. The court further observed that "[a]lthough NCMEC is not officially a government entity, it receives a grant from the government, and one of the uses to which NCMEC puts this grant money is to operate the CyberTipline and forward reports of child pornography to law enforcement." Id. at 644 (citing 42 U.S.C. § 5773(b)(1)(P)). The "partnership" between NCMEC and law enforcement with respect to the operation of the CyberTipline is not just rhetorical but real. Members of law enforcement serve on various NCMEC boards, and U.S. Marshals and other law enforcement personnel provide on-site support and referral assistance for NCMEC's Exploited Child Division. As noted above, NCMEC makes the results of its examination of suspected files available exclusively to federal and state law enforcement officials by means of a dedicated VPN, accessible only to law enforcement personnel. It is clear that NCMEC's CyberTipline is, and is intended by Congress to be, an integral part of the governmental effort to detect and prosecute child pornography crimes. Cf. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 615 (1989) (holding that drug testing was not a private search where the "Government has removed all legal barriers to the testing . . . and indeed has made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions").

If AOL had sent the file directly to the FBI or the State Police instead of to NCMEC's CyberTipline, it could not seriously be contended that the law enforcement agency could open and inspect the contents of the file without regard to the Fourth Amendment's warrant requirement.[4] See Walter v. United States, 447 U.S. 649

[4] The Fourth Amendment forbids "unreasonable" searches. Ordinarily, and especially in the criminal context, a search is not "reasonable" under the Fourth Amendment unless it has been authorized in advance by a warrant issued upon probable cause. See Payton v. New York, 445 U.S. 573, 586 (1980). However, the Supreme Court has held that in certain cases there may be an exception to the requirement of a warrant, "where 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement

(1980). In Walter, a package containing boxes of film was mistakenly delivered to a private company. The company's employees opened the package and saw that the individual boxes bore outside labeling suggesting that they contained obscene material. They notified FBI agents, who took custody of the boxes, opened them, and viewed the films, confirming what the outside labeling suggested. Id. at 651-52. The Court held that the opening and viewing of the films by the FBI was an expansion of the private search that required a warrant. Id. at 660. Although the media in which criminally obscene material was stored are different in Walter and this case, the pattern is the same. A label (here, hash value) that is examined without opening the film or file suggested the nature of the contents. For that reason, concerned private parties provided the film or file to the government without first reviewing the contents themselves. Government personnel then examined the contents of the film or file by opening and viewing it. Walter holds that the examination should not have been done without due compliance with the warrant requirement imposed by the Fourth Amendment. The only possibly significant difference between the circumstances in Walter and here is that instead of a direct employee of the FBI or State Police performing the examination, an outside contractor performed the examination for the benefit of the law enforcement agency. There is nothing wrong with the government outsourcing part of its investigative work to a private cooperating partner, but doing so does not avoid the obligation to abide by the requirements of the Fourth Amendment.

The government weakly argues that a NCMEC analyst's viewing of the contents of the file was not an expansion of AOL's private search, citing United States v. Jacobsen, 466 U.S. 109 (1984). In that case, FedEx employees opened a damaged box for private, non-governmental reasons, discovered what appeared to be cocaine, and contacted the Drug Enforcement Administration. The FedEx employees put the contents back in the box. When DEA agents arrived, they reopened the package and removed the cocaine. Id. at 111. In these

---

impracticable.'" Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (citation omitted). In such cases, other means than the warrant requirement may adequately serve to protect Fourth Amendment interests. See Donovan v. Dewey, 452 U.S. 594, 598-99 (1981). The government has not argued that the "special needs" exception to the warrant requirement could or should be applicable here, and accordingly I do not consider that question.

circumstances, the Supreme Court held there had been no separate search by the police to which the Fourth Amendment applied. Id. at 120. An argument that Jacobsen is factually similar to this case is untenable in light of the testimony given at the evidentiary hearing. It is indisputable that AOL forwarded the suspect file only because its hash value matched a stored hash value, not because some AOL employee had opened the file and viewed the contents. The NCMEC analyst expanded the review by opening the file and viewing (and evaluating) its contents. Walter, and not Jacobsen, is the better analog.

In this regard it is worth noting that matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it. That is surely why a CyberTipline analyst opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in Jacobsen, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search. Jacobsen is inapposite.

## V. New Hampshire Investigation of the Staples Laptop

On July 29, 2010, employees in a Staples store in Plaistow, New Hampshire alerted local police that a laptop computer left for repair contained files with filenames suggesting that they contained child pornography. It does not appear that the Staples employees actually viewed any of the files. The work order for the Staples laptop listed the defendant's name and Haverhill address. On August 10, 2010, a Plaistow police officer questioned the defendant, who admitted both that the Staples laptop was his and that he had seen and downloaded upwards of fifty files depicting images of children as young as eight years old engaging in sexual activity. The officer then applied for and obtained a state warrant to search the laptop. According to the affidavit

of Massachusetts State Trooper Michael Murphy submitted in support of his application for the warrant for the search at issue here, the forensic examination of the laptop pursuant to the New Hampshire warrant revealed online chat messages suggesting possible sexual abuse of a minor living in the defendant's house. Police independently confirmed that the minor in question did live there. The search also discovered a photographic image of the defendant in the vicinity of computer equipment other than the laptop. The Plaistow police contacted the Haverhill police who contacted Trooper Murphy, conveying the information from the investigation of the laptop.

## VI. The Application for and Execution of the Search Warrant

Trooper Murphy applied for the warrant for the search at issue here relying on both the NCMEC CyberTipline reports and evidence from the Staples laptop investigation. A warrant issued, and Massachusetts State Police executed it on September 17, 2010, recovering physical evidence the government expects to be useful in the present prosecution. The defendant also was advised of his Miranda rights and questioned. Again, he made statements admitting to the possession of child pornography.

The defendant contends that because Trooper Murphy's affidavit relied on information obtained in violation of the Fourth Amendment by NCMEC in the course of its CyberTipline examination of the suspect file, the application was tainted by unlawfully obtained information and the search warrant was improperly issued. He further argues that if the CyberTipline information is excluded, the affidavit does not sufficiently establish probable cause for the search of his residence. I disagree.

There was a sufficient factual basis to support probable cause if only the information from the investigation of the Staples laptop were to be considered. Paragraphs 10 through 12 of Trooper Murphy's affidavit present facts from the laptop investigation. Those facts include that Staples personnel had discovered possible files containing child pornography on a laptop, that the Staples work order named the defendant as the owner of the laptop and gave a Haverhill address that other information independent of the CyberTipline report

indicated was the defendant's address, that in a subsequent interview with Plaistow police the defendant "admitted that the Toshiba laptop referenced above is his and that he has seen and downloaded images of children as young as 8 years old engaged in sexual activity," that a forensic examination of the computer at the request of the Plaistow police "recovered multiple online chat messages with various individuals discussing the possible sexual abuse of a child living in the home of David Keith," that it was independently confirmed that a child with the same name used in the chats did reside there, and that a recovered photograph showed the defendant in proximity to computer equipment other than the searched laptop. (See Def.'s Mem. in Supp. of Mot. to Suppress Evidence, Ex. 3 ("Search Warrant Affidavit") at 6-7 (dkt. no. 23-3).) Based on these facts, the magistrate could properly have determined that probable cause existed that evidence of computer based child pornography crimes could be found at the Keith residence. Moreover, although the record may not be entirely clear on this point, Trooper Murphy's affidavit indicates that he attached the affidavit that Sergeant Caggiano of the Plaistow police had submitted to a New Hampshire court to obtain a warrant to search the laptop. That affidavit supplies further specifics, including the highly suggestive names of some of the files on the laptop. (See id., Ex. 4 at 3-4 (dkt. no. 23-4).)

I also conclude that the State Police would have applied for the warrant solely on the basis of the information from the laptop investigation. The CyberTipline report and others like it had been received several months earlier. While police opened and apparently continued an investigation into those reports, they did not move to seek a search warrant based on them. The laptop investigation was the more immediate impetus for the search. In particular, the forensic examination done on the laptop revealed information that there might be a child living in the defendant's home in immediate danger of actual sexual abuse. The timeline is also significant. Trooper Murphy apparently learned of the results of the forensic exam of the laptop computer either on September 16 or 17, and he applied for the warrant on the 17th. This rather strongly suggests that the

"proximate cause" (as it were) of the application was the specific information provided as a result of the laptop investigation, and not the earlier CyberTipline reports.

The information from the New Hampshire investigation was not stale, contrary to the defendant's contention. That investigation had begun less than two months before. There is no standard measurement for assessing whether information is stale for these purposes. The affidavit set forth Trooper Murphy's assertion that his training and experience with child pornography crimes (detailed in the affidavit) teach that in general "[t]hose who have demonstrated an interest or preference in sexual activity with children or in sexually explicit visual images depicting children are likely to keep secreted, but readily at hand, sexually explicit visual images depicting children," that "persons trading in, receiving, distributing, or possessing images or movies involving child pornography will make copies of those files on their computer's hard drive or other removable media," and that "even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner." (See id., Ex. 3 at 7.) There was evidence that the defendant possessed on his laptop files likely constituting child pornography at the end of July. These quoted assertions from Trooper Murphy's experience supported a conclusion that it was probable that a search in mid-September would yield evidence of at least past, if not present, possession of similar images. In light of that evidence, the photograph of the defendant in the presence of other computer equipment was sufficient to support a finding by the magistrate that it was probable that such equipment was located at the defendant's residence.

Accordingly, I conclude that if the evidence presented in the affidavit from the NCMEC search were to be excised from the affidavit, there was nonetheless a sufficient factual basis set forth, based on the laptop investigation, for the magistrate to have concluded that the issuance of the requested warrant was adequately supported by probable cause.

## VII. Good Faith and the Exclusionary Rule

Evidence obtained in violation of the Fourth Amendment may not be used against a defendant in a criminal prosecution. Weeks v. United States, 232 U.S. 383, 398 (1914). The exclusionary rule, however, is not a remedy for a completed private wrong, but a practical means of deterring future unlawful behavior by agents of the government. United States v. Calandra, 414 U.S. 338, 347 (1974). The Supreme Court has observed that "[t]he deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct" to deprive a defendant of a guaranteed right. United States v. Peltier, 422 U.S. 531, 539 (1975) (internal quotation marks omitted). As a corollary, the Court has concluded that the deterrent effect of exclusion of evidence is minimal where an officer has acted on an objectively reasonable belief that his actions did not violate the Fourth Amendment. United States v. Leon, 468 U.S. 897 (1984). In Leon, the Court concluded that the exclusionary rule should not be applied to prevent the use in a criminal prosecution of evidence obtained by officers whose reliance on a warrant issued by a magistrate was objectively reasonable, even though it was later determined that probable cause for the issuance of the warrant was lacking. "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." Id. at 921.

In Leon, the officers acted in objectively reasonable reliance on a warrant issued by a magistrate.[5] The Court has also held that the exclusionary rule should not be applied to suppress evidence obtained by officers who acted in objectively reasonable reliance on a statutory scheme that authorized warrantless administrative searches, even though the statute was later found to violate the Fourth Amendment. Illinois v. Krull, 480 U.S. 340 (1987). That is similar to this case. Congress has by statute given NCMEC's CyberTipline a significant role in the investigation and subsequent prosecution of child pornography crimes, and has directed that it be

[5] I have concluded that the Murphy affidavit contained a sufficient basis for a finding of probable cause to search the defendant's residence even if the NCMEC information were disregarded and only the information from the laptop investigation were considered. If that conclusion is wrong and the warrant was improperly issued, nonetheless the reliance of the State Police on the warrant was objectively reasonable under Leon, and the evidence should not be excluded.

supported by government grants. While I have concluded that NCMEC conducts its CyberTipline program as an agent of law enforcement so that its inspections of the content of emails are subject to the Fourth Amendment, it still must be acknowledged that those who heretofore regarded NCMEC's role only as that of a private party, so that the Fourth Amendment was inapplicable, were not acting in willful or negligent disregard of constitutional principles, but rather pursuant to a view of NCMEC's statutorily sanctioned role and activity that was, under all the circumstances, objectively reasonable, just as the officers' view of the statutory scheme was found to be in Krull. In that case the Court explained that "evidence should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." Krull, 480 U.S. at 348-49 (internal quotation marks and citation omitted).

There is nothing in the record in this case that would suggest either NCMEC or the police or the magistrate who issued the warrant knew or ought to have known that by relying on the CyberTipline report they were doing something that was unconstitutional under the Fourth Amendment. No persuasive argument can be made that an organization like NCMEC needs to be deterred from acting in good faith in a way that is consistent with explicit congressional will.

Moreover, any possible deterrent value from applying the exclusionary rule must be weighed against the "substantial social costs" of suppressing the evidence. See Leon, 468 U.S. at 907; see also Herring v. United States, 555 U.S. 135, 141-42 (2009). The Supreme Court has cautioned that the exclusionary rule

> almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a "last resort."

Davis v. United States, -- U.S. --, 131 S. Ct. 2419, 2427 (2011) (internal citations omitted). In this case, where the likely deterrent value of exclusion is so minimal, the balance tips decidedly against suppression.

## VIII. Summary

To summarize my major conclusions as to contested issues:

1. In monitoring its network email traffic using its Image Detection and Filtering Process, AOL was acting for its private purposes, and the Fourth Amendment did not apply.

2. In examining the contents of the emailed image file from the defendant's computer that was uploaded to its CyberTipline server, NCMEC was acting as an agent of federal law enforcement, and the Fourth Amendment applied.

3. Accordingly, NCMEC's examination of the contents of that emailed image file violated the Fourth Amendment because it was not authorized by a duly issued warrant (or by some constitutionally adequate substitute).

4. Probable cause for the issuance of the search warrant in this case was nevertheless adequately supported by facts in the affidavit concerning the defendant's laptop, and the warrant would more likely than not have been applied for and issued even if no information from the CyberTipline had been included in the affidavit. For this reason, the Fourth Amendment violation by NCMEC did not affect the validity of the warrant.

5. Even if the Fourth Amendment violation by NCMEC were deemed to have affected the validity of the warrant, considering all the circumstances, the exclusionary rule should not be applied to suppress the fruits of the search.

For all the reasons set forth above, the defendant's Motion to Suppress Evidence (dkt. no. 22) is DENIED.

It is SO ORDERED.

/s/ George A. O'Toole, Jr.
United States District Judge

**Publisher Information**

**Note* This page is not part of the opinion as entered by the court.**

**The docket information provided on this page and following pages is for the benefit of publishers of these opinions.**

1:11-cr-10294-GAO All Defendants USA v. Keith

Date filed: 08/31/2011

Date of last filing: 11/05/2013

Attorneys

Charles P. McGinty

Federal Public Defender Office

District of Massachusetts

51 Sleeper Street

5th Floor

Boston, MA 02210

617-223-8061

617-223-8080 (fax)

charles_mcginty@fd.org

Assigned: 09/21/2011

TERMINATED: 11/16/2011

ATTORNEY TO BE NOTICED representing David A. Keith (1) (Defendant)

Eve A Piemonte-Stacey

U.S. Attorney's Office

1 Courthouse Way

Suite 9200

Boston, MA 02210

617-748-3100

617-748-3969 (fax)

eve.stacey@usdoj.gov

Assigned: 11/07/2012

ATTORNEY TO BE NOTICED representing USA (Plaintiff)

Suzanne M. Sullivan

United States Attorney's Office

1 Courthouse Way

Suite 9200

Boston, MA 02210

617-748-3146

617-748-3951 (fax)

suzanne.sullivan@usdoj.gov

Assigned: 08/31/2011

ATTORNEY TO BE NOTICED representing USA (Plaintiff)

Timothy G. Watkins

Federal Public Defender Office

District of Massachusetts

51 Sleeper Street

5th Floor

Boston, MA 02210

617-223-8061

617-223-8080 (fax)

timothy_watkins@fd.org

Assigned: 09/21/2011

ATTORNEY TO BE NOTICED representing David A. Keith (1)

(Defendant)